

PRE-APPEAL BRIEF REQUEST FOR REVIEW

(filed with the Notice of Appeal)

Docket Number 042023/294057

**RECEIVED
CENTRAL FAX CENTER**

Application Number: 09/944,694

Filed August 31, 2001

APR 03 2006

First Named Inventor: Matthew Gast

Art Unit: 2135

Examiner: Leynna A. Ha

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.


This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

Attachment: Remarks (five (5) pages)

Respectfully submitted,


Andrew T. Spence
Registration No. 45,699

Date

4/3/06

Customer No. 00826

ALSTON & BIRD LLP

Bank of America Plaza

101 South Tryon Street, Suite 4000

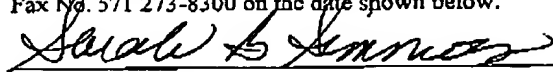
Charlotte, NC 28280-4000

Tel Charlotte Office (704) 444-1000

Fax Charlotte Office (704) 444-1111

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the US Patent and Trademark Office at
Fax No. 571 273-8300 on the date shown below.


Sarah B. SimmonsApril 3, 2006
Date

CLT01/4809086v1

In re: Gast
Appl. No.: 09/944,694
Filed: August 31, 2001

REMARKS

This communication is filed in response to the final Official Action of November 1, 2005, and the Advisory Action of February 13, 2006. The final Official Action and Advisory Action reject Claims 1 and 2 under 35 U.S.C. § 112, first paragraph, alleging that the specification of the present application fails to support amendments to those claims presented in response to the first Official Action. In addition, the final Official Action and Advisory Action further reject all of the pending claims of the application, namely Claims 1-18, under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,772 to Binding et al. As explained below, Applicant again respectfully submits that the specification does in fact support the claimed invention, and that Claims 1-18 are patentably distinct from Binding. In view of the remarks presented herein, Applicant respectfully requests reconsideration and reversal of the rejections to the claims.

A. Claims 1 and 2 are Supported by the Specification

The final Official Action and Advisory Action allege that the specification of the present application does not support the following limitation of Claims 1 and 2: "at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network layer protocol." To the contrary, however, Applicant respectfully submits that the specification does in fact support the aforementioned limitation. As disclosed in the specification at paragraph 24 and with reference to FIGS. 3 and 4, a network protocol packet 204 may include a network protocol header 402 and network protocol data 404. The network protocol data in turn may include a first cryptographic protocol header 406 and a first plurality of encrypted data 408. In one disclosed example embodiment, the cryptographic protocol header 406 may comprise a TCP header, which is well known to those skilled in the art as a transport layer protocol. See Wikipedia, *Transmission Control Protocol – Wikipedia, the Free Encyclopedia* (last modified Dec. 29, 2005)

<http://en.wikipedia.org/wiki/Transmission_Control_Protocol> (explaining that "TCP does the task of the transport layer in the simplified OSI model of computer networks."). In another example embodiment, the cryptographic protocol header 406 may comprise an ESP header, which as is well known to those skilled in the art, is a network layer protocol. See Wikipedia, *IPSec – Wikipedia, the Free Encyclopedia* (last modified Nov. 2, 2005)

In re: Gast

Appl. No.: **Error! Reference source not found.**

Filed: August 31, 2001

<<http://en.wikipedia.org/wiki/IPSec>> (explaining that the IPSec standard includes the ESP protocol, which operates at layer 3 – i.e., the network layer – of the OSI model).

Applicant therefore respectfully submits that at least at paragraph 24 and FIGS. 3 and 4, the specification of the present application discloses a cryptographic protocol header (i.e., a portion of a network protocol packet) being configured in accordance with TCP (i.e., a transport layer protocol) or ESP (i.e., a network layer protocol). Accordingly, Applicant also respectfully submits that the specification of the present application does in fact include the aforementioned limitation of Claims 1 and 2; and respectfully request that the rejection of Claims 1 and 2 under 35 U.S.C. § 112, first paragraph, be reversed.

B. Claims 1-18 are Patentable

As explained in response to the first Official Action, Binding discloses a piggy-backed key exchange protocol for providing low-overhead browser connections from a client to a server using a trusted third party. According to one disclosed scenario implementing the disclosed system, a client sends the server a common HTTP message (e.g., HTTP GET) that includes security-sensitive parameters encrypted using scheme M1 (i.e., parameters \rightarrow M1[parameters]). The server, being unable to process the encrypted parameters, encrypts the encrypted parameters using scheme M2 (i.e., M1[parameters] \rightarrow M2[M1[parameters]]), and forwards the further-encrypted parameters to a trusted third party (TTP). Being configured to process messages encrypted with either scheme M1 or scheme M2, the TTP decrypts the further-encrypted parameters using scheme M2 (i.e., M2[M1[parameters]] \rightarrow M1[parameters]), and then decrypts the encrypted parameters using scheme M1 (i.e., M1[parameters] \rightarrow parameters), the decryption steps resulting in cleartext parameters (i.e., parameters). Thereafter, the TTP re-encrypts the cleartext parameters using scheme M2 (i.e., parameters \rightarrow M2[parameters]), and forwards the re-encrypted parameters to the server. The server decrypts the re-encrypted parameters using scheme M2 to similarly obtain the cleartext parameters (i.e., M2[parameters] \rightarrow parameters).

Generally, in contrast to the claimed invention's handling of security at the transport layer (e.g., TCP/UDP) or the network protocol layer (e.g., IP), Binding provides a system and method for providing security at the application layer (e.g., HTTP). More particularly, in contrast to the method of independent Claim 1, Binding does not teach or suggest performing

In re: Gast

Appl. No.: **Error! Reference source not found.**

Filed: August 31, 2001

cryptographic operations (i.e., determining cryptographic rules, establishing a cryptographic session, applying the cryptographic rules, etc.) based on network protocol packets at least a portion of some of which are configured in accordance with a transport layer protocol or a network layer protocol. In addition, Binding does not teach or suggest translating a first plurality of cleartext data into a second plurality of cleartext data, as also recited by independent Claim 1.

I. Network Protocol Packets

Binding discloses that transport-based security protocols such as WTLS (see Claim 6) and SSL (see Claim 9) are ineffective in environments having transcoders and gateways that must inspect and thereafter modify some non-security-sensitive sections of a data stream. As also disclosed, to enable an intermediary to perform content modifications, end-to-end security must be provided at the application layer. Binding Patent, col. 3, lines 3-24. Accordingly, Binding discloses a system and method that establishes and maintains end-to-end security sessions at the application layer, while maintaining the integrity of an application-layer protocol and avoiding adding amounts of communication and message exchanges. *Id.* at col. 4, lines 9-14. More particularly, as indicated above, Binding discloses that a client piggy-backs security-sensitive parameters onto application-layer message headers, such as common HTTP message (e.g., HTTP GET) headers. In contrast, the claimed invention recites that at least a portion of some of the received network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP). Thus, whereas the Binding system operates at the application layer of the OSI model protocol stack, the claimed invention operates at the transport layer or network layer of the protocol stack.

The Advisory Action alleges that Binding discloses using TCP, citing column 6, line 65 – column 7, line 3. In this regard, Applicant does recognize that Binding discloses workstations connecting to a wireless network, and the wireless network connecting to another network, using TCP/IP. Even in such an instance, however, Binding does not teach or suggest cryptographic operations being performed on network protocol packets at least a portion of which is configured in accordance with TCP, similar to the claimed invention. Although packets may be communicated over TCP/IP, as explained above the cryptographic operations of Binding are not performed at the TCP/IP layer. Rather, as disclosed by Binding, cryptographic operations are

BEST AVAILABLE COPY

In re: Gast

Appl. No.: **Error! Reference source not found.**

Filed: August 31, 2001

performed at the application layer. The claimed invention, on the other hand, recites performing cryptographic operations (i.e., determining cryptographic rules, establishing a cryptographic session, applying the cryptographic rules, etc.) at either the transport layer or the network protocol layer (or based on based on network protocol packets configured in accordance with such layer protocols).

2. Cleartext Translation

As explained in response to the first Official Action, the cited passage of Binding (column 15, lines 52 – 59) discloses a TTP encrypting security-sensitive parameters using scheme M2, where a server from which a client requested content later decrypts the parameters and uses them to create the requested content that can then be encrypted and provided to the client. Binding therefore discloses creating requested content based upon security-sensitive parameters. Binding does not disclose, however, translating a first plurality of cleartext data into a second plurality of cleartext data. More particularly, even if it could reasonably be suggested that the disclosed security-sensitive parameters and requested content correspond to a first and second plurality of cleartext data, respectively, Binding can not reasonably be interpreted to teach or suggest translating the security-sensitive parameters into the requested data, as recited by the claimed invention.

In response to the foregoing remarks, the final Official Action and Advisory Action allege that any form of decoded data being re-encrypted, and then again decoded to second decoded data, as disclosed by Binding, meets the respective limitation. In the aforementioned instance, the first decoded data is the same as the second decoded data (i.e., parameters → parameters). In the claimed invention, however, the first plurality of cleartext data is translated to a second plurality of cleartext data that is different from the first cleartext data. Applicants note that the claims of the present application do not explicitly recite that the first and second plurality of cleartext data are different, but the typical meaning of the recited term “translating” and logic dictate such an interpretation. In this regard, the term “translating” is well understood to those skilled in the art as meaning to change from one form to another. In fact, even in the cited passage of Binding, each instance of translating or encoding/decoding involves those steps being performed to move the data from one form (encoded/decoded) to another (the other of

BEST AVAILABLE COPY

In re: Gast

Appl. No.: **Error! Reference source not found.**

Filed: August 31, 2001

encoded/decoded). The entire sequence, however, does not translate first cleartext data to another, second cleartext data. Further, any individual operation in the sequence also does not translate first cleartext data to second cleartext data, since the individual operations either start or end with encoded, and not cleartext, data (i.e., parameters \rightarrow M1[parameters] or M1[parameters] \rightarrow M2[M1[parameters]] or M2[M1[parameters]] \rightarrow M1[parameters] or M1[parameters] \rightarrow parameters or parameters \rightarrow M2[parameters] or M2[parameters] \rightarrow parameters).

Applicant therefore respectfully submits that the method of independent Claim 1, and by dependency Claims 4-11, is patentably distinct from the system and method of Binding. Applicant also respectfully submits that independent Claims 2 and 3, and by dependency Claims 12-18, recite subject matter similar to that of independent Claim 1, with independent Claims 2 and 3 each individually reciting one of the aforementioned features. As such, Applicant respectfully submits that independent Claims 2 and 3, and by dependency Claims 12-18, are patentably distinct from Binding for at least those reasons explained above with respect to independent Claim 1.

C. Dependent Claims 6 and 9

In addition to the aforementioned reasons, Applicant respectfully submits that various ones of dependent Claims 4-11 recite features that are further patentably distinct from the system and method of Binding. For example, dependent Claims 6 and 9 further recite that the first and second cryptographic protocols comprise WTLS and SSL over HTTP, respectively. As will be appreciated, and as explained in Binding, WTLS and SSL are both transport-layer security protocols. As also explained by Binding, however, such protocols have drawbacks in certain environments, which Binding seeks to overcome by establishing and maintaining end-to-end security sessions at the application layer. Thus, although Binding does disclose the existence of the WTLS and SSL protocols, Binding teaches away from their use by implementing its disclosed application-layer security system and method.

Applicant therefore respectfully submits that Claims 1-18 are patentably distinct from Binding. Accordingly, Applicant also respectfully submits that the rejection of Claims 1-18 under 35 U.S.C. § 102(e) as being anticipated by Binding is overcome.